双**WAN**口宽带路由器

使用说明

Ver:1.0

目录

物　品　清　单

小心打开包装盒，检查包装盒里应有以下配件：

一台路由器
一条电源线
一张产品说明光盘
一张保修卡

注意

如果打开包装时发现产品有所损坏或者任何配件短缺的情况，请及时和当地经销商联系。

第一章　用户手册简介(Introduction)

感谢您购买本公司的双 WAN 口企业网吧路由器。双 WAN 口企业网吧路由器具备有 2 个 WAN 连接端口，允许多台计算机共享 2 条宽带同时连接因特网，几倍于普通路由器的带宽。可混合使用不同的因特网连接方式，如 Cable Modem，ADSL，ADSL PPPoE，LAN PPPoE，光纤等网络接入，也可以接入不同 ISP 线路，满足您不同需求。通过线路负载均衡设置将两条宽带连接达到最高效。

双 WAN 口企业网吧路由器是为您提供高度的网络安全和网络资源共享的产品。由于它包含强大的防火墙引擎，所以能够防御网络攻击，同时因为包含了数据包过滤，可以防止用户的私人网络免受因特网黑客袭击。还能通过 IP 流量控制实现对内网用户的外网资源控制，让您的网络更加稳定快捷。

双 WAN 口企业网吧路由器还能通过内网 IP+MAC 绑定防御 ARP 病毒，使您的网络更加安全稳定。另外，还能通过数据包策略控制实现内网的管理，让不同的用户拥有不同的权限，在企业网络管理中能够发挥其重要的作用。

通过基于 WEB 页面管理来进行配置 ，此双 WAN 口企业网吧路由器易于安装和维护。所有的功能均可通过网络浏览器来进行配置。

本产品除了具有高效能的传输速率之外，更结合简易的设置接口，让用户在使用上本产品只需要极短的时间，便能完成基本的设置步骤，让用户使用起来更轻松更方便。

1.1　用途

本手册的用途是帮助您熟悉和正确使用双 WAN 口企业网吧路由器。

1.2　约定

在本手册中所提到的路由器，指此双 WAN 口企业网吧路由器。

1.3　用户手册概述

第一章：　用户手册简介。
第二章：　产品概述。简述路由器的主要特性和规格。
第三章：　硬件安装。帮助您进行路由器的硬件安装。
第四章：　配置指南。帮助您配置路由器的基本网络参数和高级特性。

第二章　产品概述

感谢您购买多 WAN 口企业网吧路由器。本手册将会帮助您正确的安装、使用本产品。

2.1　产品简介

企业网吧宽带路由器专为企业和网吧用户设计，采用 Intel IXP 网络专用处理器，基于 Intel XSCale 技术，主频最高达 533MHz，多 CPU 分布式处理，性能优越，并内置高冗余电源模块，充分保证整机的稳定可靠。

此系列企业网吧宽带路由器除支持宽带路由器常见的功能外，还支持带宽控制、系统安全日志等高级功能，内建先进防火墙功能，可防止 DoS 攻击、扫描、嗅探式攻击，有效防止 Nimda、冲击波、木马等病毒攻击，能灵活指定 IP、用户或应用分配带宽和设定优先级，保证特殊用户、特殊应用（如 VoIP 等）的服务质量，全中文配置界面，配置简单，全面满足企业、机关、大型网吧、大型宽带社区、校园网等对网络的高性能、多功能、高可靠性、高安全性的需求。

2.2　产品特性和规格说明

2.2.1　产品特性

- 采用 Intel IXP 533MHz 网络专用处理器，多 CPU 分布式处理
- 支持 2 个 WAN 口接入，支持 4 个 LAN 口
- 符合 IEEE802.3、IEEE 802.3u、IEEE 802.3x
- 支持 TCP/IP、NAT、DHCP、FTP、PPPoE、PPTP、HTTP、TFTP
- 支持静态路由表更新及升级功能
- 支持流量管理和 IP 流量控制
- 支持虚拟服务器、静态路由表等功能；可以有针对地开放指定计算机的上网权限
- 内建防火墙，支持 IP 地址过滤、MAC 地址克隆和 IP、MAC 地址绑定，提供安全日志和流量控制
- 支持 WEB 远程管理，全中文配置界面，支持在线升级
- 内置优质开关电源，稳定可靠
- 1U 超大全钢外壳，支持标准 19 英寸机架安装

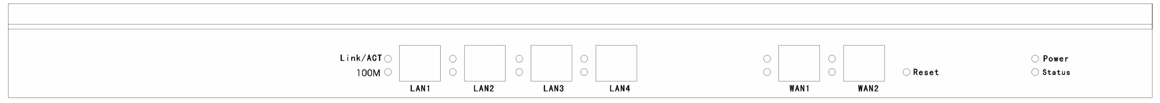
2.2.2　规格

产品型号		高性能双 WAN 口路由器
支持的标准和协议		IEEE802.3、IEEE802.3u、IEEE802.3x、TCP/IP、FTP、PPPoE、PPTP、HTTP、TFTP、DHCP、NAT、IPSec
端口	WAN	2
	LAN	4
网络介质		10Base-T:3 类或 3 类上 UTP　100Base-T：5 类 UTP
过滤和转发速率		10Mbps:14880pps；　100Mbps:1448800pps
LED 指示	WAN	Link/Act(连接/工作)、100M
	LAN	Link/Act(连接/工作)、100M
	其它	M1（系统灯），Power（电源）
外形尺寸（L×W×H）单位（mm）		440×290×44
使用环境		工作温度：0ºC 到 40ºC；工作湿度：10%到 90%不凝结 存储温度：-40ºC 到 70ºC；存储湿度：5%到 90%不凝结
输入电源 功耗		输入：220VAC，50Hz 功耗：最大 15W

第三章　硬件安装

3.1 面板布置

3.1.1　前面板



图：前面板示意图

LED 灯号说明

LED	描述	意义
Power	电源状态指示灯	绿灯常亮：　电源开启连接
Status	系统状态指示灯	绿灯常亮：路由器非正常工作 绿灯闪烁：路由器工作正常
Link/Act	端口连接/传输指示灯	绿灯常亮：以太网络联机正常 绿灯闪烁：以太网络端口正在传送/接收封包数据传输
100M	端口 100M 传输速率指示灯	绿灯常亮：以太网络端口传输速率为 100M

3.1.2　后面板

交换机后面板有一个电源接口。电源工作范围：180-260V～50Hz-60Hz。



图：后面板示意图

➢ 电源插座

这是一个二相三线电源插座，把电源线阴性插头接到这个插座上，阳性插头接到交流电源上。

提示： 如果您忘记了路由器的密码或**IP**地址，您可通过此按钮恢复出厂设置。路由器通电状态下，按住此按钮**10**秒以上，直到**Status**灯常亮后，松开按钮，即可恢复出厂设置。

3.2 连接到您的网络上

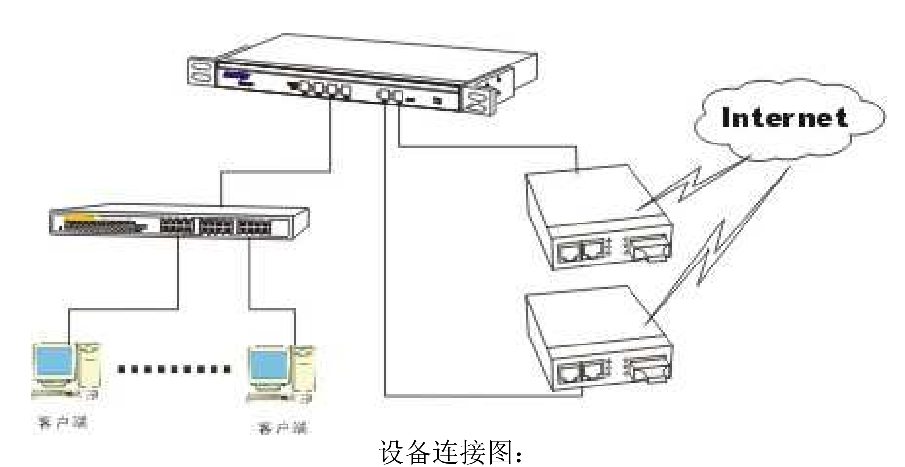
首先，请您参考以下步骤完成双 WAN 口企业网吧路由器的网络连接。

1)　建立局域网连接

用一根网线连接路由器的 LAN 口和局域网中的集线器或交换机。您也可以用一根网线将路由器 LAN 口与您的计算机网卡直接相连。

2)　建立广域网连接

用两根网线连接路由器和 xDSL Modem／Cable Modem 或以太网。



设备连接图：

3) 连接电源

将电源连接好，路由器将自行启动。

第四章　　配置指南

4.1 概　述

本路由器采用 WEB 方式进行管理。用户可以使用 WEB 浏览器登录路由器，友好、直观的管理界面将让您觉得配置路由器是一件轻松的事。

4.2　　WEB 管理的连接

4.2.1　　准备工作

首先，必须确保管理电脑安装了网页浏览器软件(比如 Microsoft Internet Explorer，简称 IE)，而且浏览器必须支持 JavaScript 脚本功能。由于不同的浏览器对网页代码的解释不尽相同，为保证配置操作的准确无误，建议您使用微软的 Internet Explorer 浏览器，如果您使用 Netscape 浏览器，请确保其为最新版本。如果您使用 Internet Explorer 浏览器，请确保其版本在 5.0 以上，建议使用 6.0 版本。为了达到良好的浏览效果，建议您将显示分辨率设为 1024×768 或者更高。

如果您在配置本宽带路由器的时候，WEB 页面不能正常使用或者不能正常配置路由器，需要按照以下的说明来初始化操作系统的浏览器配置。一般情况下如果能够正确配置路由器的话，不需要更改浏览器的设置，此时请跳过以下几步。

为了使 WEB 方式的管理能正常进行，我们需要对所使用的网页浏览器软件进行配置，下面以 Windows XP 下 IE 6.0 为例说明。

第一步在 IE 菜单中选择“工具”→“Internet 选项”，会弹出 Internet 选项对话框：



图：Internet 选项设置

第二步：点击“删除文件”，清除浏览器的缓存记录；特别需要时点击“删除 Cookies”清除自动登录记录（慎用）。

点击“设置”按钮，进入设置对话框，如下图所示：



图：设置对话框

如果您使用 Internet Explorer 5.0 版本的浏览器，请您务必选择“每次访问此页时检查”一项。否则将可能导致某些页面显示的路由器配置信息错误。

如果您使用 Internet Explorer 6.0 版本的浏览器，可以选择“每次访问此页时检查”项或“自动”项，建议选择后者。

选择完成后点击“确定”按钮即可。

注　意：

选择“每次访问此页时检查”项将使 Internet Explorer 浏览器在每次刷新时都会从路由器取完整的页面文件，而不是读取磁盘中的临时文件。这将保证配置信息的正确无误，但同时也可能导致页面的显示速度变慢。如果您选择了此项，在完成对路由器的 WEB 配置后，将其改为“自动”一项，否则您访问其它网页时显示速度将可能受到较大影响。Internet Explorer 6.0 对此问题处理较好，可以放心使用“自动”项(默认选项)。

第三步：请选择 Internet 选项对话框的“安全”标签，然后点击“自定义级别”按钮，如下图所示：



图：Internet 选项设置

第四步如果上述操作正确无误，就会弹出以下的对话框：



图：安全设置

请选择活动脚本中的“启用”或者将“重置”下拉文本框设置成“安全级-中”，点击“重置”按钮，最后点击“确定”按钮。

第五步：在桌面上单击鼠标右键，选择弹出菜单中“属性”选项，将弹出显示属性对话框，如下图所示：



图：分辨率设置

请选择“设置”标签，将屏幕区域设置为 1024×768，并单击“应用”按钮。如果修改分辨率后感觉屏幕较为闪烁，请单击上图的“高级”按钮，在弹出窗口的“监视器”页面中调高显示刷新率，具体细节此处略过。

经过了以上设置，您就可以畅通无阻地通过 WEB 对交换机进行配置了。

注意：

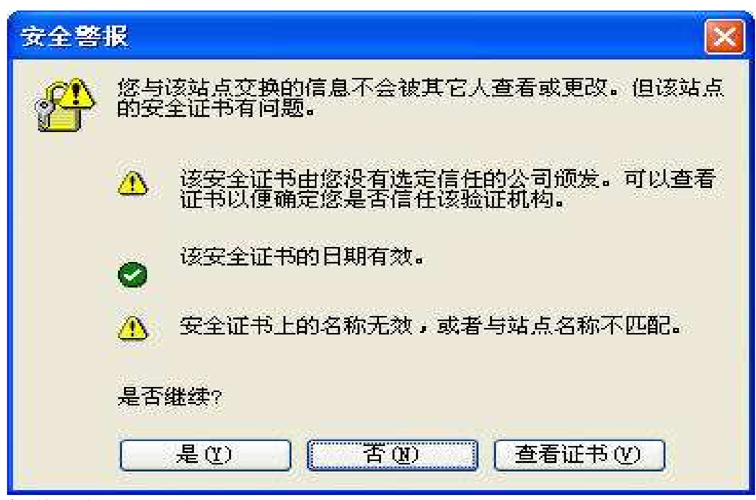
将屏幕的分辨率设为 1024×768 是对 PC 硬件设备有一定要求的，对于硬件配置较低的 PC 可以不按此设置。

4．2．2　连接

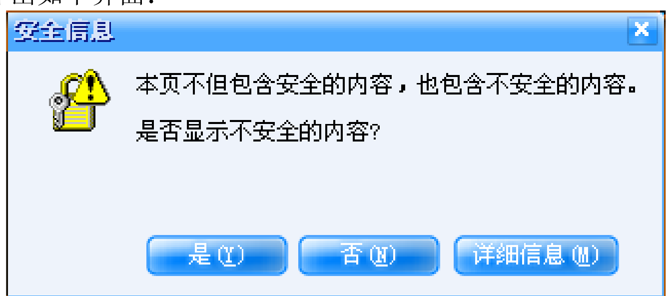
将的LAN口用一根网线连到本地的交换机上，再通过一台普通PC的网卡连接到交换机上；或是直接联到一台普通PC的网卡接口上。将该PC的网卡IP地址设为192.168.0.X（X为1～253）网段，掩码为255.255.255.0，即可进行首次登陆。

在 IE 的地址栏输入 https://192.168.0.254:10000 打开管理界面登陆。

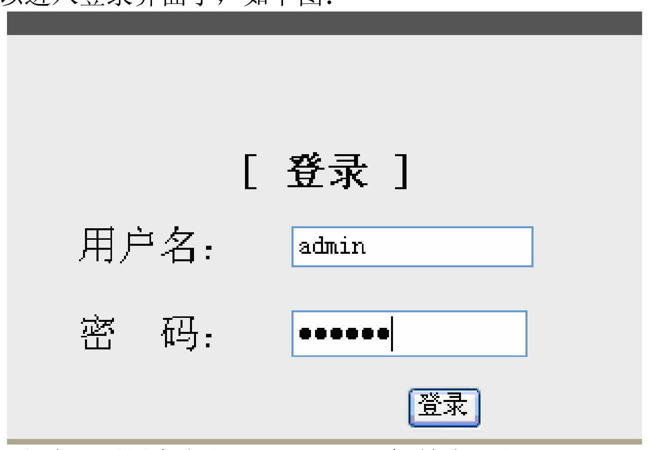
在进入登录界面前会弹出如下对话框，



点击“是”，会弹出如下界面：



点击“是”，就可以进入登录界面了，如下图：



默认登陆界面用户名是“admin”，初始密码是“888888”。

在指定的用户名和密码输入框中输入用户名和密码，点击“登录”按钮，就进入 WEB 管理路由器主页了。

注 意：

路由器的缺省密码是 出厂时设置的。您也可以在路由器的修改帐号设置页面中修改密码。为了安全，我们强烈建议您务必在登录之后更改管理密码！密码请牢记，若是密码忘记，将无法再登录至路由器的设定画面，必须恢复到出厂值。

4.3 WEB管理界面及操作方法

在页面左侧，本公司商标的正下方，是功能菜单界面，它呈树状目录结构；右下方大面积的区域是用于功能配置的主窗口。



左侧的功能菜单呈树状目录结构，整个目录分成两层，如果点击某一主项，就会展开这一主项下的所有子项；如果想要设置其子项，只需要点击相应子选项，主窗口就会切换到被点击子项的设置页。

在一个主项被展开的情况下，如果点击其它主项，以前展开的主项会闭合，被点击的主项将展开，此时主窗口仍然会显示上一次设置的子项的设置页，只有点击了新的设置子项，配置页面才会更改；如果点击已打开的主项，此主项会闭合，此时没有打开的主项，主窗口仍然会显示上一次设置的子项的设置页。由于受到网络速度和路由器工作负荷影响，可能菜单会将两次间隔时间较短的点击作一次点击来响应，此时只要注意适当延长点击时间间隔即可。



图：功能菜单

以下列出了功能菜单以及其子项：

系统信息：无

网口配置：模式选择、WAN1 口配置、WAN2 口配置、内网配置

网络配置：内网 DHCP、DNS 和 DDNS 配置、静态路由设置、VLAN 设置、内网 IP 绑定

防火墙：设置选项、时间表、 IP 管理、服务、端口映射、IP 地址映射、数据包控制策略、会话列表

VPN 配置：PPTP 设置、PPTP 用户

流量管理：IP 流量控制

服务管理：时间设置、命令行工具、系统升级、配置备份与恢复、恢复默认值

配置向导：无

系统日志：无

修改帐号：无

重新启动：无

退出： 无

注意：

针对路由器设置所做的修改，只有在点击“保存”按钮（有些项目可能还需要路由器系统重启）后才会生效。

4.3.1 系统信息



- 系统信息：主要显示系统的相关信息如软件版本、以及当前的DDNS主机名、系统当前时间。
- 端口信息：显示内网的IP以及WAN口IP以及端口的所有信息如内网、外网的流入、流出数据包的数据量。
- 资源状态：显示本路由器的资源信息。

注意：

系统信息中的系统时间只有在“服务管理”中的“时间设置”项中正确设置后才能反映正确时间。

4.3.2 网口配置

在“接口配置”菜单下面，有“模式选择、WAN1 口配置、WAN2 口配置、内网配置”四个子项。单击某个子项，您即可进行相应的功能设置，下面将详细讲解各子项的功能。

4.3.2.1 模式选择

4.3.2.1.1 路由模式

选择路由模式，假如和其它的路由器同在一个网络上运作，这里包括了一个分别处理上网的网关，假如选择路由模式，您需要设置另一个路由器作为网关，以便让接入路由的电脑也能够上网。此时，本路由器不具备NAT功能。

您当前的位置是：模式选择

模式

路由模式

透明桥模式

IP地址

子网掩码

外置网关

带宽(kbit/s)：上行 下行

NAT模式

网关模式

自动负载均衡（多路ADSL时启动）

重 启 保存

注意：1.当您网络设置为透明模式时，将清除原先的LAN/WAN口IP设置。
2.模式选择改变后，必须重启系统，新设置才能生效。

点击“保存”按钮保存选择的路由模式。使配置生效必须重新启动本机，点击“重启”按钮，等待重启完成，重新连接才能进入配置界面。

4.3.2.1.2 透明桥模式

透明桥模式是用来连通两个大型的网络。您的网络管理人应该填入网络段的信息，包括IP地址，子网掩码，和外置的网关地址。设置成透明桥模式，您的路由器将没有WAN口和LAN口之分。而且能够通过带宽限制来限制您的此设备下面设备的总流量带宽。

您当前的位置是：模式选择

模式

路由模式

透明桥模式

IP地址

子网掩码

外置网关

带宽(kbit/s)：上行 下行

NAT模式

网关模式

自动负载均衡（多路ADSL时启动）

重 启 保存

注意：1.当您网络设置为透明模式时，将清除原先的LAN/WAN口IP设置。
2.模式选择改变后，必须重启系统，新设置才能生效。

- IP地址： 所有的WAN口和LAN口会分享这个IP地址。
- 子网掩码：所有的WAN口和LAN口会在这个子网里。
- 外置网关：外置网关指的是已在网络内部运行且被设置为网关的设备。
- 带宽：
  - 上行带宽：此 WAN 口分配上行数据的速率。路由器默认值为 102400kbps(100M)。这一配置对上行数据缓存调节和权重来说很重要。如果您使用上行速率为 0.5Mbps 的 DSL 服务，那么上行速率设置为 500K bit/s。
  - 下行带宽：此 WAN 口分配下行数据的速率。路由器默认值为 102400kbps(100M)。这一配置对下行数据缓存调节很重要。如果您使用下行速率为 2Mbps 的 DSL 服务，那么下行速率设置为 2000K bit/s。

点击“保存”按钮保存选择的透明桥模式。使配置生效必须重新启动本机，点击“重启”按钮，等待重启完成，重新连接才能进入配置界面。

4.3.2.1.3 网关模式

一般的宽带连接使用网关模式。自动负载均衡是在多路ADSL情况下启用的，此选项能够自动均衡两个外网数据的流入，内网到外网的数据也能进行合理的分配，使得网络资源更加合理的得到利用。

您当前的位置是：模式选择

模式

路由模式

透明桥模式

IP地址

子网掩码

外置网关

带宽(kbit/s)：上行　　下行

NAT模式

网关模式

自动负载均衡（多路ADSL时启动）

重　启　保存

注意：1.当您网络设置为透明模式时，将清除原先的LAN/WAN口IP设置。
2.模式选择改变后，必须重启系统，新设置才能生效。

点击“保存”按钮保存选择的网关模式。使配置生效必须重新启动本机，点击“重启”按钮，等待重启完成，重新连接才能进入配置界面。

4.3.2.2　WAN1口配置

设定WAN1口的配置信息。先选择WAN口的配置方式，然后再输入对应的参数即可。

您当前的位置是： WAN1口配置

WAN1口的配置方式:

- 静态IP
- ADSL拨号连接
- DHCP连接
- 关闭连接

静态IP配置选项:

IP地址	192.168.0.23	DNS服务器1	
网络掩码	255.255.255.0	DNS服务器2	
默认网关	192.168.0.254	DNS服务器3	

(如果不设置DNS服务器,系统将不进行断线检测)

拨号连接配置选项

登录用户名		登录密码	
从ISP得到DNS配置?	是 否	尝试连接的时间	60 秒(40-90)
是否限制包尺寸?	1412 字节	是否进行LCP检测?	是 否

WAN1 静态路由:

分行填写，格式如20.10.10.0/24

上行带宽: kbit/s 下行带宽: kbit/s

使用DNS查询检测断线: MAC地址克隆

保存配置 (重新启动后生效)

重 启

- WAN 口的配置方式：用户可以根据自己的方式进行选择“固定 IP、ADSL 拨号连接、DHCP 连接、关闭连接”。
- 静态 IP 配置选项： 静态 IP 时，由 ISP 提供相应的 IP 地址，DNS 必须手动填写。
- 拨号连接配置选项： ADSL 拨号连接，连接时的用户上网账号和密码由当地 ISP 提供商提供。
  - 登陆用户名：输入当地 ISP 提供商提供的用户名。
  - 使用密码登陆：输入当地 ISP 提供商提供的密码。
  - 从 ISP 得到 DNS 配置：选择是否要从 ISP 处自动获得 DNS 服务器。
  - 尝试连接时间：尝试连接时间一栏默认设置为 40 秒（取值 40 到 90 之间）。若选择了尝试连接的时间选项且使用默认设置，PPPoE 连接就从开始拨号 40 秒如果没有连接上，就会开始新的 PPPoE 进程。

- ✧ 是否限制包尺寸：选择是否限制包尺寸选项。
- ✧ 是否进行 LCP 检测：ADSL 的断线检测。

- DHCP 连接：直接由 ISP 提供商进行动态的 IP 地址分配。
- WAN1 静态路由：显示手动设置的 WAN1 口的静态路由表项，静态路由的表达格式为：202.104.25.33/16，前者为目的 IP 地址或网段，后面为 32 分段表达方式子网掩码，16 对应的子网掩码为 255.255.255.0（可以参考说明书最后部分的分位表示法的表格）。
- 带宽管理：
  - 上行带宽：此 WAN 口分配上行数据的速率。路由器默认值为 102400k bps(100M)。这一配置对上行数据缓存调节和权重来说很重要。如果您使用上行速率为 0.5Mbps 的 DSL 服务，那么上行速率设置为 500K bit/s。
  - 下行带宽：此 WAN 口分配下行数据的速率。路由器默认值为 102400k bps(100M)。这一配置对下行数据缓存调节很重要。如果您使用下行速率为 2Mbps 的 DSL 服务，那么下行速率设置为 2000K bit/s。

  提示：带宽管理只有在选用流量管理中的最小带宽管理才可生效。（搭配使用）
- 断线检测：对于静态 IP 和 DHCP（动态 IP）接入方式如果需要检测连接状态，可以选择此项。
- MAC 地址克隆：可以更改路由器 WAN 口的 MAC 地址。

以上配置只有在重启后才能生效。

小知识：

什么是 DNS？

DNS 是域名系统 (Domain Name System) 的缩写，该系统用于命名组织到域层次结构中的计算机和网络服务。DNS 命名用于 Internet 等 TCP/IP 网络中，通过用户友好的名称查找计算机和服务。当用户在应用程序中输入 DNS 名称时，DNS 服务可以将此名称解析为与之相关的其他信息，如 IP 地址。因为，您在上网时输入的网址，是通过域名解析系解析找到相对应的 IP 地址，这样才能上网。其实，域名的最终指向是 IP。

比如您在浏览器中输入 www.163.com，那么 DNS 服务器将会将此域名解析成类似于 218.107.213.22 的 IP 地址，由于 ISP 的服务差异，使得每次解析结果都不一定相同。

4.3.2.3 WAN2口配置

WAN2口配置与WAN1口配置相同，此处略。

4.3.2.4 内网配置

LAN 口地址配置及网段参数；依照用户需求设定。示例：

您当前的位置是：内网配置列表

接口名称	IP地址	子网掩码
内网（编辑）	192.168.10.254	255.255.255.0

☑ 广播arp信息(防止arp欺骗) 速度 2 个/秒(1-30)

☐ 在LAN口启动snmp服务

确定

点击“内网”输入路由器的 IP 地址和子网掩码。

- IP地址：路由器对于内网的IP地址。
- 子网掩码：内网的IP掩码。

点击“保存”按钮保存设置。使配置生效必须重新启动本机，等待重启完成，重新连接按照更改后的IP地址才能进入配置界面。

- 广播ARP信息（防止ARP网关欺骗）：每秒钟发送一次网关的IP与MAC地址信息广播包。为了保证局域网中的电脑不被感染病毒和木马的电脑欺骗，可以选中此项，使得每台电脑能获得正确的网关信息。
- 在LAN口启用snmp服务：启用此服务能够在LAN的PC中启用SNMP管理路由器。

注意：

此处设置的路由器内网IP必须与第4.3.3.1内网DHCP章节中设置的网关IP保持一致。

小知识：

什么是ARP?

ARP（Address Resolution Protocol，地址解析协议）是一个位于TCP/IP协议栈中的低层协议，负责将某个IP地址解析成对应的MAC地址。从影响网络连接通畅的方式来看，ARP网关欺骗主要分为二种，一种是对路由器ARP表的欺骗；另一种是对内网PC的网关欺骗。

第一种ARP网关欺骗的原理是——截获网关数据。它通知路由器一系列错误的内网MAC地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的MAC地址，造成正常PC无法收到信息。第二种ARP网关欺骗的原理是——伪造网关。它的原理是建立假网关，让被它欺骗的PC向假网关发数据，而不是通过正常的路由器途径上网。在PC看来，就是上不了网了，“网络掉线了”。

上面已经说了，ARP网关欺骗形式有对路由器ARP表的欺骗和对内网PC的网关欺骗两种，我们的防护当然也是两个方面的，首先在路由器上进行设置，来防止路由器的ARP表被恶意的ARP数据包更改，通过IP与MAC地址的绑定来实现，如在内网DHCP设置中的“自动应用于绑定MAC地址的IP用户”（第4.3.3.1章节）和内网IP绑定设置中手动设置内网IP与MAC地址的绑定（第4.3.3.5章节）；其次，我们也可以通过广播网关IP与MAC的正确信息来防止对内网PC的网关欺骗，如内网配置中的广播ARP信息（第4.3.2.4章节）。

4.3.3 网络配置

4.3.3.1 内网DHCP

DHCP服务器默认值是开启的，开启DHCP服务器功能可以提供局域网络内的计算机自动取得IP的功能，（如同NT服务器中的DHCP服务），好处是每台PC不用去记录与设定其IP位置，当计算机开机后，就可从路由自动取得IP地址，管理方便。

您当前的位置是： DHCP配置列表

☑ 打开DHCP服务

☐ 自动应用于绑定MAC地址的IP用户

网关IP		(可选)
DNS服务器		(可选)
内网IP地址起点	192.168.10.10	
内网IP地址终点	192.168.10.250	
内网IP网络掩码	255.255.255.0	

确定

- 打开DHCP服务器：开启DHCP功能，使路由器作为DHCP Server为局域网自动分配IP地址。
- 自动应用于绑定MAC地址的IP用户：此选项可以使得在DHCP服务打开时，PC的MAC地址和所获取的IP有确定关系，而不是递加和随机的，直接保存在IP+MAC地址绑定中（第4.3.3.5章节）。
- 网关IP：该设置为路由器对局域网的IP地址。该IP地址出厂设置为**192.168.0.254**，用户可以根据需要改变它。
- DNS服务器：手动输入DNS服务器地址后，DHCP服务器将此DNS服务器地址分配给PC。
- 内网IP地址起点：该设置为路由器的DHCP服务器为局域网内电脑分配IP地址时开始的值，若设置为192.168.0.2.也就是说，第一台向路由发出申请的电脑，获取的IP是192.168.0.2，第二台则会是192.168.0.3.依此类推。如果需要，您可以改变该数值。
- 内网IP地址终点：该设置为路由器的DHCP服务器为局域网内电脑分配IP地址时最后的值。若设置为192.168.0.150，则IP地址从开始值分配至此值时，即不再分配IP地址。
- 内网IP网络掩码：该设置为路由器对局域网的子网掩码。

注 意：

1. 为了使用本路由器 DHCP 功能，局域网中计算机的 TCP/IP 协议必须设置为“自动获取 IP 地址”。
2. 设置完成后，请点击“确定”按钮使用户的设置生效。
3. 当WAN处于拨号模式且没有从ISP处获取DNS服务时，可在此处填入DNS服务器地址，且需与“DNS&DDNS配置”中DNS服务器设置第一栏保持一致。
4. “自动应用于绑定MAC地址的IP用户”功能启用后，会将路由器下所带设备的IP与MAC地址对应表记录在（第4.3.3.5章节）内网IP绑定设置的ARP列表中。

4.3.3.2 DNS&DDNS配置

DDNS（动态DNS）服务让您分配一个固定的网域名给一个动态WAN IP地址。

在还没有设置 DDNS 之前，您需要访问 WWW.DTDNS.COM， WWW.3322.org 或其它的 DDNS 服务商并且注册一个网络域名。（DDNS 服务是 DTDNS.COM 等服务商提供的）在其中的动态域名当中添加一个您当前网络的主机名。然后在这里将对应的信息填写进去。

DDNS 服务：在默认下 DDNS 功能是没有启动的。要激活此功能，只要从下拉式菜单中选择一个 DDNS 服务商，并且在您和 DDNS 服务商设置的帐户里输入用户名，密码，和主机名。

选择启动 DDNS 后，每次拨号连接都会自动更改本域名的 IP 地址，则客户端即可通过动态域名访问到服务器。

您当前的位置是： DNS 配置

DNS 客户选项

DNS 服务器 202.96.134.133
202.96.128.166

动态DNS选项

动态dns服务商
主机名
DDNS的用户名
DDNS的密码
是否启动 是 否

确定

- DNS服务器：输入IP地址到DNS服务器1栏，如果连接成功这个DNS IP地址会先被采用。 输入IP地址到DNS服务器2和3栏作为备份。DNS服务器2会被采用如果无法连接上DNS服务器1。然后以此类推，DNS服务器3会被采用如果DNS服务器1和2都无法连接上。
- DDNS动态服务商：可以选择3322.org、dtdns.com、congle.com、vier.cn、webddns。
- 主机名：向DDNS服务提供者所申请的本设备的主机名称，如：router123.3322.org。
- DDNS的用户名：向DDNS所注册的账号用户名。
- 密码：向DDNS服务提供者所申请的与用户名名称对应的密码。
- 是否启动：点击“是”将启动此选项，点击“否”将不启动此选项。
- 确定：按下此按钮“确定”即会储存刚才所变动的修改设定内容参数。

小知识：

何谓 DDNS 服务？

所谓 DNS 是域名解析服务器的意思，即把域名转换成为网络可以识别的 IP 地址，使得互联网用户可以通过名称访问这个 IP 所指向的服务。对于通过 ADSL 上网的电脑而言，每次上网的时候有不同的 IP 地址，一般无法通过 DDNS 将域名固定指向这个固定的电脑。而 DDNS 服务（动态域名解析服务）就是把域名与这个动态的 IP 地址对应起来。

DDNS 的用途是什么？

简单而言，DDNS 可以将您的电脑变成一个互联网上的用户都可以访问的服务器，不过这个服务器是在您的家中或者单位里罢了。使用 DDNS 让您的电脑可用于：

- Web 服务器——发布自己的网站并不受限制
- Mail 服务器——构建自己的邮件服务器收发邮件
- FTP 服务器——文件的上传或者下载
- VPN 服务器——不需要固定 IP 就可实现企业网之间的连接
- 远程访问服务器——随时随地管理自己的电脑

DDNS 如何实现？

需要一个能够提供 DDNS 服务的服务商，以便能够为您提供 DNS 解析服务。当您的 IP 发生变化的时候，能够立刻更改域名的指向，外网的用户都访问您新的 IP 所指向的电脑。其次，您的电脑上需要安装一个客户端软件，能够在您的电脑的 IP 地址发生变化的时候通过 DDNS 服务器进行新的解析服务。

本宽带路由器的 DDNS 服务就是在路由器上内置了对应的客户端软件，使得用户在宽带路由器内部不需要客户端软件就能享受 DDNS 服务。

4.3.3.3 静态路由设置

通过配置静态路由，用户可以人为地指定对某一网络访问时所要经过的路径， 在网络结构比较简单，且一般到达某一网络所经过的路径唯一的情况下采用静态路由。

假如好几个路由器连接到您的网络，为了确保您方便快捷的与那几个路由器所在网络的通讯，您会需要配置静态路由。静态路由的功能决定数据在您网络上流动的路线。静态路由让不同的IP网域用户经过路由访问Internet。这是一个高级的功能，请小心地进行。

您当前的位置是：静态路由

目的地IP	子网掩码	默认网关	操作

页码：1/0 上一页 下一页 新 增

点击“新增”按钮增加一个路由表格。输入下面的数据，创立静态路由表格：

您当前的位置是：新增静态路由

填写静态路由

目的地IP

子网掩码

默认网关

保存 取消

- 目的地IP：输入远距离LAN 分段的网络地址。
- 子网掩码：输入目的地LAN IP网域的子网掩码。基于Class C IP 网域标准，子网掩码是255.255.255.0或其他设定的值。
- 默认网关：假如路由是用来连接网络到互联网，那么网关的IP是路由的LAN IP地址。

点击：“保存”按钮保存静态路由设置。

4.3.3.4 VLAN设置

这里所谓的VLAN，就是在单个网络接口上绑定多个虚拟接口和不同的网段。也就是说，被VLAN隔离的用户可以同时接到单个网络接口，在经过网关上网访问的同时，也可以在不同的VLAN之间彼此互访。因为在用户上网的同时可以成为VLAN用户之间互访的桥梁，额外的网络接口就不需要了。

您当前的位置是： VLAN设置

网络地址	子网掩码	网络接口	操作

页码：1/0 上一页 下一页 新增

点击“新增”按钮增加VLAN设置。输入下面的数据，创立新的VLAN设置：

您当前的位置是：新增VLAN设置

修改信息

网络地址

子网掩码

网络接口 透明桥

透明桥
WAN1
WAN2
LAN

保存 取消

- 网络地址：输入本地网络地址。
- 子网掩码：输入本地子网掩码。
- 网络接口：从下拉式菜单中选择一个端口透明桥、LAN，WAN1或WAN2。

点击“保存”按钮保存VLAN 设置。

4.3.3.5 内网IP绑定

用户可以在LAN口上绑定多个内网IP地址和其对应的MAC地址，还可对绑定IP进行增减操作，在绑定的IP栏里面可以查看IP对应的绑定地址。有效的防御了ARP病毒，也方便了网络管理者对内网的管理。

您当前的位置是：内网IP绑定

启 用

绑定的IP

设置内网绑定MAC地址的IP，格式如：

192.168.2.2
00:0C:29:A9:F9:AC

表示192.168.2.2绑定到00:0C:29:A9:F9:AC，IP和MAC之间以空格隔开，每行一条。点击下面的“ARP命令列表”按钮可扫描出当前的IP-MAC，以便参考和复制。

arp列表

允许新用户连接

保存

点击“ARP列表”

1、在输出列表当中填写需要绑定MAC地址的IP地址。

2、IP和MAC之间以空格符号分开每行一条。



输入完毕之后，点击“保存”按钮保存列表。

说明：

实现路由器下所带设备IP与MAC地址绑定的步骤：

1. 添加IP与MAC地址对应表（ARP列表）。对于路由器下所带设备的IP与MAC地址对应表我们可以手动添加，也可以通过路由器自动添加。
   - 手动添加：在“绑定的IP”栏中手动输入MAC与IP的对应列表。
   - 自动添加：点击“ARP列表”就可以显示出所有路由器下所带设备的IP与MAC地址对应表，复制这个列表到“绑定的IP”栏中。
2. 点击“内网IP绑定”中的“启用”按钮就可以把ARP列表中的IP与MAC实现一对一的绑定。
3. 允许新用户连接：当您不选择此项时，如果您在内网新接入一台PC，如果改PC没有进行IP+MAC绑定，那么它是无法上外网的；如果选择了此项，那么新接入的PC就可以上外网。

4.3.4.防火墙

4.3.4.1 设置选项

从防火墙功能的一般设定选项当中，您可以控制开启(Enable)或是关闭(Disable)这些选项功能。

您当前的位置是：防火墙配置

防攻击 选项

☑ 过滤 SYN 攻击	阀值: ____ 包/每秒		已过滤 : 0 包
☐ 过滤 UDP 攻击	阀值: ____ 包/每秒		已过滤 : 包
☑ 过滤 Ping of Death 攻击	阀值: ____ 包/每秒		已过滤 : 包
☑ 过滤 Tear Drop 攻击			已过滤 : 包
☑ 过滤 IP Spoofing 攻击			已过滤 : 166 包
☑ 常见攻击特征防范			已过滤 : 包
☐ 禁止本机被外网Ping			
☐ 禁止本机被外网访问			
☐ 限制非授权用户访问路由器(通过策略控制)			
☑ 限制用户每秒新建连接数	最大: 30	(10-40)	已过滤 : 50 包
☐ 限制每个用户并发会话数	最大: ____	(100-400)	已过滤 : 包
☐ 打开告警日志			
☐ 启动UPNP功能			
日志服务器地址:	____		

确定

- DOS 保护

  为了保护内网，在这里您可以设定阻止从 Internet 来的攻击，例如 SYN 攻击，UDP 攻击，Ping of Death 和 Tear Drop 等，并设置相应参数。

- IP攻击

  IP Spoofing：即 IP 欺骗。

- 常见攻击特征防范

  过滤常见的攻击包，例如根据tnk2k，ddoser等的指纹特征进行防范。

- 禁止本机被外网ping及禁止本机被外网访问

  前者选择后外网ping路由器的WAN口IP无法ping通，后者无法通过WAN口IP访问管理路由器。

- 限制非授权用户访问路由器（通过策略控制）

  在没有选择此项时，无论您在数据包控制策略中做任何设置，内网的任何PC都能进入路由器的WEB管理。在选择此项之后，您可以通过数据包控制策略来授权部分用户能管理路由器，部分用户不能管理路由器。

- 限制用户最大连接数

  在我们用电脑工作时，打开的一个窗口或一个 Web 页面需要建立 IP 连接，每一个 IP 连接我们可以把它叫做一个“会话”，扩展到一个局域网里面，所有用户要通过防火墙上网，要打开很多个窗口或 Web 页面（即多个会话），那么，这个防火墙，所能处理的最大会话数量，就是“并发连接数”。

  限制单个用户的并发连接数是为了防止病毒伪装“会话”而造成对网关的攻击。默认的最大单个用户的并发连接数是 300。

- 打开告警日志

  选择此项后，日志中会报告非法的错误的网络信息。

- 启动UPNP功能
  选择此项后，路由器能够实现自动的端口映射。
- 日志服务器地址：在日志服务器地址栏中填入日志服务器的IP就可以保存路由器中的日志，；路由器重启后在PC上也能保存，为以后的查询工作，解决问题提供便利。

说明：

防火墙的设置相对复杂，而且对于网络性能的影响也比较大，因此我们以网吧环境为参照提供部分参数的设置。

对于网吧，必须要设置的内容：

1、最大连接数：保证不会出现由于病毒、木马、BT等P2P软件占用太多的系统资源，由于常见的软件的会话数小于50，所以建议：网吧设置为200－300之间比较合适，较宽裕的环境设置为400－600。

2、打开防火墙，但是不要设置UDP包过滤，不然容易引起QQ、网络游戏不能正常使用。

防攻击 选项

过滤 SYN 攻击 阀值: 5000 包/每秒 已过滤： 包

- 过滤 UDP 攻击 阀值: 包/每秒 已过滤： 包（一般网络情况不要采用 ）
- 过滤 Ping of Death 攻击 阀值：200 包/每秒 已过滤: 包
- 过滤 Tear Drop 攻击 已过滤: 包
- 过滤 IP Spoofing 攻击 已过滤 ： 0 包
- 常见攻击特征防范 已过滤 ： 0 包
- 禁止本机被外网Ping
- 禁止本机被外网访问
- 限制非授权用户访问路由器(通过策略控制)
- 限制每个用户并发会话数 最大： 200 已过滤： 包

注意:

在日志服务器地址栏中填入日志服务器的IP之外，还必须在PC上安装一个日志信息接收端。

4.3.4.2 时间表



时间表是服务于防火墙中的数据包控制策略的，在数据包控制策略中，您可以通过定义时间表来实现数据包控制策略只在某一个时间段实现。具体时间表分为以下两种，可以点“增加”来进行添加：

您当前的位置是：新增时间表

名称

启用循环操作　开始时间 00 时 00 分　结束时间 00 时 00 分　星期 星期一 星期二 星期三 星期四 星期五 星期六 星期日

启用单次操作　时段起始于 1970 年 01 月 01 日 00 时 00 分 00 秒　时段终止于 1970 年 01 月 01 日 00 时 00 分 00 秒

说明：1.当各选项为空时，表示不限制；2.循环和单次操作可以相互组合。　保存

- 名称：定义此条时间表格的名称，在数据包控制策略中可以选择到您定义的时间表。
- 启用循环操作：以星期为单位，按星期一至星期天每天的时间来定义时间段，循环操作。
- 启用单次操作：以时间起始定义时间表，从1970至2037年内的任意时间段，单次操作。

4.3.4.3 IP管理

对用户名及IP等进行定义，方便管理，也可以在数据包控制策略中对您所定义的IP及IP段进行策略控制。可以定义一个用户，也可以定义一组用户，一段IP用户，也可以定义单个域名或者外网IP。用户定义后即可针对该用户设定相应的防火墙规则。当所定义的用户已被防火墙规则使用时，要删除该用户必须在删除对应防火墙的规则后，才可被删除。下图为本说明示例：



点击“创建”可新建用户，点击用户名可以对已有的原用户进行编辑：

您当前的位置是：新增IP

修改信息

名称*

○ 单个IP
IP地址 [*]
子网掩码 255.255.255.255
MAC地址

单击"*"按扭，选arp命令列表中的值，再点击，可变为可填写状态。

○ 一组IP
IP地址
子网掩码

○ 一段IP
起始IP
终止IP

⊙ 其他IP或域名

可填写的形式有两种，如：
A. 192.168.1.23
B. www.google.com
可以添加达2000个以上IP，适用于批量地址处理

保存

网络掩码可以表示一段地址，也可以表示一个地址，而MAC码表示一个地址。当表示一个地址时，可以和MAC地址一起用。输入MAC 地址时需要用冒号"："隔开。

4.3.4.4 服务

对网络端口进行定义，以便于管理。可以定义数个端口，也可以定义一段连续的端口。端口定义后即可针对该用户设定相应的防火墙规则。当针对端口设定了相应的防火墙规则后，则不能再直接删除所定义的端口，如需删除，需先删除定义的规则。

在这里，端口的定义分为缺省和手动2部分，缺省为不能更给的，系统已经定义好的端口。在手动中，您可以定义一些您需求的端口或者端口段。下图为本说明示例：

您当前的位置是：服务

缺省 手动

序号	服务名	端口范围	协议	操作
1	NetMeeting	1720	TCP/UDP	
2	PPTP	47,1723	TCP/UDP	
3	SNMP	161-162	TCP/UDP	
4	NTP	123	TCP/UDP	
5	UDP	0-65535	TCP/UDP	
6	QUAKE	26000,27000,27910,27960	TCP/UDP	
7	AOL	5190-5194	TCP/UDP	
8	INFO_ADDRESS	17	TCP/UDP	
9	IKE	500	TCP/UDP	
10	HTTPS	443	TCP/UDP	

页码：1/5 [1] 跳转 上一页 下一页

您当前的位置是：新增服务

服务设置

服务名 * | 协议 TCP/UDP

端口号 ◉ 起始 0 终止 65535 （端口范围）

○ 第1个 第2个 第3个 第4个 第5个 第6个 第7个 第8个 第9个 第10个 （单个填写，至少填写第一个）

保存

- 服务名：您所定义的服务名称
- 端口号：您可以定义一个端口段（起始-终止）
  组合的端口号组（可以是一个或者多个）

4.3.4.5 端口映射

端口映射用于建立web 站点、Email、FTP 服务器等服务。

端口映射功能被用来在网络上设置公共服务。当在您网络外的用户（Internet上的用户）向您的网络提出请求，能转发那些请求到已装备好处理这些请求的电脑。例如说，您转发端口号80（HTTP）到IP地址192.168.1.1，那么所有从外而来的HTTP请求会被转发到192.168.1.1。

您可以使用此功能经由IP网关建立Web站点、Email、FTP服务器等服务。例：将192.168.1.1的Server 端口80映射为WAN口公网IP的8080端口，您就可以通过http://WAN的IP：8080来访问192.168.1.1这台PC上的服务器。

确定您输入了一个有效的IP地址。（为了适当地操作一个Internet服务器也许您需要建立静态的IP地址）为了增加安全，那些在您网络之外的（例如Internet）用户会能够和服务器相通，但他们事实上不会连接到服务器。那些信息包只是经过转发而已。

您可以通过修改和删除对您已经定义好的端口映射进行编辑和删除。



- 端口范围：您所定义的外网端口
- 映射端口方位：您所映射的内网服务器端口
- 服务器：空白默认为 WAN 口 IP
- 映射服务器：内网的服务器IP
- 协议：可以选择包括(TCP/UDP)

例：您在192.168.0.98这台PC上架设了FTP服务器，您只需要做如上设置，您就可以通过外网的IP来访问192.168.0.98这台PC上的FTP服务器。（服务器默认为当前的外网IP）。

4.3.4.6 IP地址映射

物理网络不能直接识别IP地址，必须经过一定的转换才能将IP地址映射为网络的物理地址。将外网的IP 地址（59.173.89.191）直接映射到内部服务器的IP 地址（192.168.0.5）让外网用户可以充分利用内部网络的资源。

您当前的位置是： IP地址映射

序号	IP地址	映射服务器	操作
1	59.173.89.191	192.168.0.5	修改 删除

页码： 1/1 　1 跳转 上一页 下一页 增加

注：如果子网掩码为255.255.255.255，则是单机用户，其他为组用户

例如：外网IP：59.173.89.191直接映射到内部服务器192.168.0.5可以充分利用网络资源，外网的用户就能通过59.173.89.191这个IP访问到内部服务器192.168.0.5。

您若要编辑IP地址映射，点击在操作栏里的“修改”按钮。也可以将其删除。

您当前的位置是：新增IP地址映射

IP地址映射

服务器IP地址*

映射服务器*

保存

提示：服务器IP地址为外网的IP地址，映射服务器填写的内网服务器IP地址。

4.3.4.7 数据包控制策略

您可以在这里通过定义不同的访问规则，来实现对内网的用户的管理，进行组合，实现内网用户不同的权限。

注意：序列号在先的规则先起作用，当检测到数据包符合某条规则后，该规则被执行，防火墙将不再检测后续规则。“内网IP”“外网IP”“服务”需要在之前的“IP管理”“服务”项中进行定义。以及访问规则中出现的“时间表”，也需要在“时间表”项中进行定义。



提示：设定了多条数据包策略后，点击“使配置生效”方可生效；且序列号越小，规则优先级越高。

例：1.您定义了一条规则，内容为内网所有用户都能上www.sina.com.cn这个网站，序列号为“001”。
2.您再定义一条规则，内容为内网所有用户都不能上外网，序列号为“002”。
此时，内网的所有用户不能上外网，但是都可以访问vwww.sina.com.cn。

您当前的位置是：新增访问规则

访问规则

☑ 启用

序列号* （序列号小则优先级高。）

日志标记 （即在该条日志上做一特殊标记，最大长度20字符。）

内容过滤 ◉数据包 ○域名 ○非标准HTTP请求 ○文件后缀名

○封锁 QQ ○封锁 MSN ○WEB行为日志

说明： 1.选“域名”时，可匹配完整或部分域名，,可以填写多个,以空格隔开；
2.选“非标准HTTP请求”时可过滤非HTTP标程序通过80端口通讯；
3.选“文件后缀名”时的填写格式如：*.bat *.exe *.doc，以空格分隔。

方向 内网->外网 内网IP 请选择 外网IP 请选择 要编辑下拉菜单的内容，请点击旁边小箭头可转到相应设置页面。

服务 请选择 IP类型 请选择 带宽控制 kbit/s

时间表 请选择

说明： 1.带宽控制，控制这条策略每个IP的最大带宽,选择时,超出带宽的包将被拒绝；
2.时间表，即此条规则只应用于所选的时间段中有效；
3.当某项不选择时，代表该项不做限制。

当以上条件符合时(策略) 通过

通过：允许该数据包通过，不记入日志
拒绝：拒绝该数据包通过，不记入日志
日志：记入日志，并继续执行下条规则
拒绝并日志：拒绝该数据包通过，并记入日志
外网线路：让该数据包走特点的外网口

注意：带*的为必填项 保存

- 序列号：序列号小则优先级高，如“001”的优先级高于“002”
- 日志标记：在“当以上条件符合时”选择到“日志”或“拒绝并日志”时，系统日志中由于此规则而出现的日志信息会有这条特殊标记，帮助区分导致此日志信息出现的原因。
- 内容过滤：当选择到“数据包”时，内容为关键字符的过滤。
  当选择到“域名”时，可以填写完成或部分的域名，可以写多个，以空格隔开。
  当选择到“非标准HTTP请求”，可以过滤非HTTP标准程序通过80端口进行通讯。
  当选择到“文件后缀名”，填写格式魏：.bat .exe .doc 中间以空格隔开。
  当选择到“封锁QQ”“封锁MSN”时，通过定义可以让内网用户不能上QQ和MSN。
  当选择到“WEB行为日志”时，可以在系统日志中看到通过WEB上网的行为日志。

- 方向：内网到外网，外网到内网，定义的是这个规则的方向。
- 内网IP：可以在这里选择到您在“IP管理”中定义的IP，IP段或者IP组。
- 外网IP：可以在这里选择到您在“IP管理”中定义的外网IP。
- 服务：可以选择任意服务项，也可以选择在“服务”中定义的项目。
- IP类型：包括 ALL，TCP，UDP。（ALL为TCP+UDP）
- 带宽控制：控制这条策略每个IP的最大带宽，当超过了带宽的数据包会拒绝。（在流量控制中的定义优先于此处的设置）
- 时间表：可以选择在“时间表”项中定义的时间表项。
- 当以上条件符合时：

选择通过，所定义的规则允许通过。
选择拒绝，所定义的规则被拒绝。
选择日志，所定义的规则将在“系统日志”中显示出来。
选择拒绝并日志，所定义的规则将被拒绝，并在“系统日志”中显示出来。
选择WAN1-WAN2，所定义的规则的数据以您所选择的WAN口作为出口

实例（此实例仅供参考，具体操作用户可灵活采用）：

如果有一家公司，用户权限分为经理，普通员工，网管。
网管的权限是可以登录路由器进行管理，能够上外网。
经理的权限是无法登录路由器进行管理，能够上外网。
普通员工的权限是无法登录路由器进行管理，不能上QQ和网页，其他一些网络服务能使用。

- 第一步：因为此处涉及到对路由器的管理，所以必须在防火墙设置选项中将“限制非授权用户访问路由器(通过策略控制)”打钩。

☑ 限制非授权用户访问路由器(通过策略控制)

- 第二步：在IP管理中定义网管，经理，普通员工3个不同的IP组，以及路由器管理IP。

您当前的位置是： IP设置

序号	名称	IP地址	子网掩码	MAC地址	操作
1	网管	192.168.0.1	255.255.255.255		修改 删除
2	总经理	192.168.0.2-192.168.0.4			修改 删除
3	普通员工	192.168.0.5-192.168.0.20			修改 删除
4	路由管理IP	192.168.0.254	255.255.255.255		修改 删除

- 第三步：实现经理及普通员工无法登录路由器进行管理，普通员工不能上QQ和网页。定义4条访问规则，分别定义经理和普通员工无法访问路由器IP，普通员工封锁QQ，普通员工封锁80端口。规则编辑如下（没指明的不更改）：

序列号：001
内容过滤：选择到数据包
方向：内网到外网
内网IP：选择经理
外网IP：选择路由器管理IP
IP类型：ALL
当以上条件符合时：拒绝

序列号：002
内容过滤：选择到数据包
方向：内网到外网
内网IP：选择普通员工
外网IP：选择路由器管理IP
IP类型：ALL
当以上条件符合时：拒绝

序列号：003
内容过滤：选择到封锁QQ
方向：内网到外网
内网IP：选择普通员工

IP类型：ALL
当以上条件符合时：拒绝
序列号：004
内容过滤：选择到数据包
方向：内网到外网
内网IP：选择普通员工
服务：选择到80端口对应的HTTP
IP类型：ALL
当以上条件符合时：拒绝

您当前的位置是：访问规则

序列号	内网IP	外网IP	服务	方向	IP类型	策略	状态	操作
001	总经理	路由管理IP		内网->外网	all	拒绝	打开	修改 删除
002	普通员工	路由管理IP		内网->外网	all	拒绝	打开	修改 删除
003	普通员工			内网->外网	all	拒绝	打开	修改 删除
004	普通员工		HTTP	内网->外网	all	拒绝	打开	修改 删除

定义以上4条规则后，就能满足上文中所提出的需求。

4.3.4.8 会话列表

您当前的位置是：会话列表

查找：0 查询 (注：只包含此字符串的会话才在下表显示。)

序号	类型	状态	源IP	源端口	目的IP	目的端口
1	udp		192.168.0.10	4185	61.147.118.194	2194
2	tcp	ESTABLISHED	192.168.0.10	1067	222.73.207.86	8080
3	tcp	ESTABLISHED	192.168.0.98	1893	203.190.122.234	80
4	tcp	ESTABLISHED	192.168.0.98	1866	202.102.57.59	80
5	tcp	TIME_WAIT	192.168.0.98	1857	121.14.95.123	80
6	udp		59.172.72.142	3164	202.103.24.68	53
7	udp		192.168.0.10	1046	207.46.48.140	3544
8	tcp	SYN_SENT	192.168.0.98	1894	61.172.240.27	80
9	tcp	ESTABLISHED	192.168.0.98	1865	202.102.57.59	80
10	tcp	LAST_ACK	192.168.0.98	1892	218.1.72.177	80
11	tcp	TIME_WAIT	192.168.0.98	1882	218.1.72.177	80
12	udp		192.168.0.98	9000	210.22.22.16	9000

页码：1/7 1 跳转 前一页 下一页

列出按会话数最多的前10条

本页显示当前的路由器的会话，您可以通过这个项目对当前所有的会话进行查看。会话分以“类型”“状态”“源IP”“源端口”“目的IP”“目的端口”来分类。您可以在查看处输入任何一个信息便可以查询到与此信息相关的所有会话。例如：您输入192.168.0.98，就会列出与此IP有关系的所有会话。

您还可以点击“列出按会话数最多的前10条”，可以查看当前会话数最多的10个IP的会话数。

按会话数降序排序的前10条

序号	源IP	会话数
1	192.168.0.98	51
2	192.168.0.10	16
3	192.168.0.11	8
4	59.172.72.142	3

刷新列表 确定

4.3.5 VPN配置

4.3.5.1 PPTP设置

用户可以设置PPTP的起始IP与终止IP，外网用户通过PPTP帐号拨进内网的时候，所获取到的IP地址段。

您当前的位置是： PPTP设置

设置

☐ 启用PPTP

起始IP

终止IP

确定

4.3.5.2 PPTP用户

您当前的位置是：新增PPTP用户

PPTP用户设置

用户名 ＊

密　码 ＊

确认密码 ＊

固定IP

保存

1: 固定IP是可选项,表示用此用户名登录则分配此IP,
注意IP地址需要在为PPTP分配的地址空间

- PPTP用户名：提供给外网拨入本路由器的PPTP用户的用户名。
- PPTP密码：提供给外网拨入本路由器的PPTP用户的密码。
- 固定IP：可以指定此PPTP用户所对应分配的IP，此IP必须在PPTP设置的IP范围内。

小提示：

PPTP：点对点隧道协议

点对点隧道协议（PPTP）是一种支持多协议虚拟专用网络的网络技术。通过该协议，远程用户能够通过 Microsoft Windows NT 工作站、Windows 98，2000，XP，VISTA的操作系统以及其它装有点对点协议的系统安全访问公司网络，并能拨号连入本地 ISP，通过 Internet 安全链接到公司网络。

4.3.6 流量控制

点击IP流量控制选项，可以输入一段IP地址进行上行和下行带宽的限制，输入完毕之后点击“保存”按钮保存生效。

您当前的位置是： IP流量控制

序号	起始IP	终止IP	上行带宽(kbit/s)	下行带宽(kbit/s)	启用
1	192.168.0.23	192.168.0.34	96	2000	☑
2	192.168.0.37	192.168.0.66	456	1232	☑
3	192.168.0.77	192.168.0.88	96	200	☑

启动队列管理： ☑

(注意，启动队列管理将降低系统性能，如果需要使用保证最小带宽时，启动队列管理，精确设置WAN口带宽，配置最小带宽的上下行值,然后重启设备生效)

流量控制方式： 保障最小带宽

(没有启动队列管理，则只有限制最大带宽生效)

保存

列出正在使用的的IP速度

- 起始IP、终止IP：此为选择您所要限制的内网IP段或者单个IP。如果只限制单个IP，只需填入：192.168.1.100 to 100，则此规则就是针对192.168.1.100 此IP 做控制。若是要限制一组IP 范

围，则填入如192.168.1.100 to 150，这样此规则就是针对192.168.1.100 到150 做限制。若是此条带宽限制是内网的所有IP 则可填入：192.168.1.0 to 0，这样就表示所有IP 都受此规则限制。

- 上行带宽：指对内网IP 的上传带宽。
- 下行带宽：指对内网IP 的下载带宽。

此处的速率为kbit/s，一般文件下载速率为KB/s，1KB=8Kb。

- 流量控制方式：
- 保障最小带宽： 如果此刻您采用的是10M光纤上网，您在外网带宽处设置下行带宽为8000kbit/s。当您下行的所有资源利用没有达到8000kb/s的时候，您的单个IP可以突破您所设置单个IP下行流量控制的数值，但是整个下行流量的总数值不会突破8000kb/s这个数值。当路由器整个下行流量的总数值达到8000kb/s，而且影响到了内网部分IP无法达到您所设置的单个IP下行流量数值的是时候，速率较高的IP的速率就会降低，能够保证内网的所有IP都能满足最小带宽。
- 限制最大带宽：为限制此条规则的最大可使用带宽，也就是最大不会超过此设定值。
- 启动队列管理：选择限制最小带宽时使用，启动队列管理将降低系统性能，如果需要使用保证最小带宽时，启动队列管理，精确设置WAN口带宽，配置最小带宽的上下行值,然后重启设备生效每台电脑的最大速度。
- 列出正在使用的IP速度：点击后可以查看当前内网IP的外网上下行流量，可以按IP，速率赖排列，能够有效的查看网络情况。

由于网吧的外网带宽是有限的，现在国内提供的有10M，20M等多种，甚至个别为100M，但是这些带宽可以完全被下载软件所占用，从而严重影响到网络的速度。因此我们首先要将外网带宽的速度设置正确。如网络的上行带宽、下行带宽要填好。根据我们在实际工作中的摸索，建议一般的网吧设置为700K bit / s以下为佳，此设置只适合于限制最大带宽的情况下。

建议：

带机量 / 带宽	100台	200台	300台
10M	<700K bit / s	<500K bit / s	<300K bit / s
20M	<700K bit / s	<600K bit / s	<500K bit / s
100M	<1000K bit / s	<700K bit / s	<600K bit / s

4.3.7 服务管理

4.3.7.1 时间设置

时间设置能将路由器的时间与用户所在时区的时间同步，方便用户管理路由器，查看系统日志，能确定出现问题所发生的时间。

您当前的位置是：系统时间

系统时间

星期	日期	月	年	时间
星期二	29	四月	2008	15 : 02 : 12

时间服务器

启用

主机/地址 210.72.145.44 时区 GMT+8

保 存

- 系统时间：此处只能查看系统当前时间。
- 时间服务器：输入NTP服务器的主机名和地址。点击“保存”按钮同步本地和NTP服务器的时间，北京时间的时间服务器IP为：210.72.145.44。
- 启用：打开或关闭从时间服务器自动获取间的开关。

4.3.7.2 命令行工具

您当前的位置是：命令行工具

输入网络工具命令

执行命令： 清理之前的命令

执行命令：在此输入您要执行的命令进行，可以执行的命令有 ping ， route ， free，ifconfig。

- ping ：此命令用于检测网络的连通。
- route ：此命令用于测试网络的路由功能和路由表。
- free：此命令用于显示内存的资源分配情况。
- ifconfig：此命令用于显示路由器的所有网络接口的连接信息和状态。

4.3.7.3 升级系统

您当前的位置是：系统升级

文件名： 浏览...

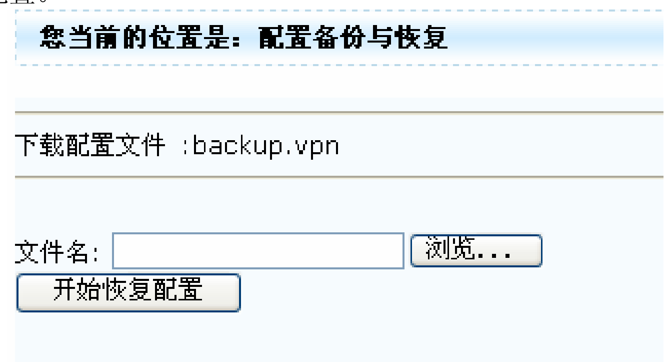
开始升级

单击“浏览”按钮选择升级文件，然后单击“开始升级”按钮，文件将被上载到设备上，升级完成后，并重新启动。

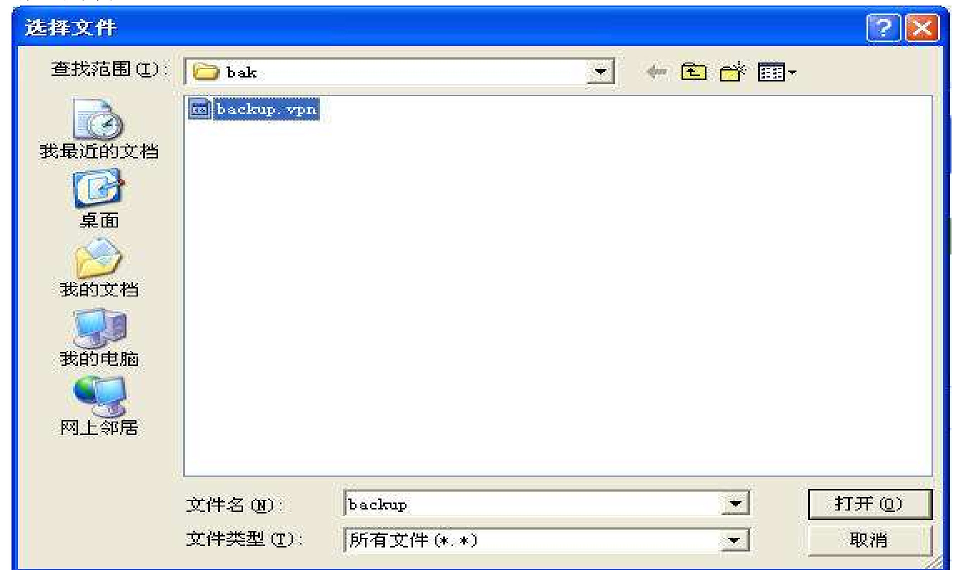
注：在升级过程中，请不要断电。升级完后介面将会自动出现“升级成功，请断电重新启动”。

4.3.7.4 配置备份与恢复

此选项可以将用户对路由器的设置进行备份。如恢复出厂设置后要恢复到用户所做的设置，可以通过此项恢复配置。



点击“backup.vpn”将路由器的配置文件保存到PC上，当需要恢复配置时点击“浏览”按钮，弹出如下界面：

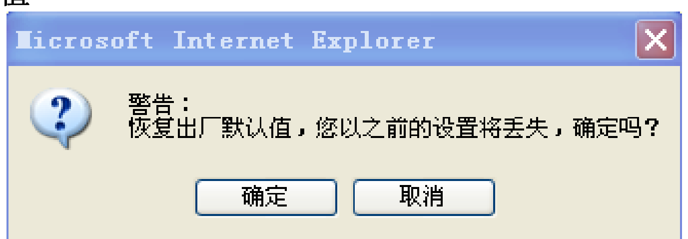


然后选择保存到PC上的配置文件，点击“打开”按钮，点击“开始恢复配置”，当弹出“恢复配置成功”的界面即可。

注意：

备份的设置最好不要包含IP与MAC地址绑定设置，因为在另一个环境恢复了包含IP与MAC地址绑定设置的配置文件，很有可能会使路由器下连的PC无法与路由器相连。

4.3.7.5 恢复默认值



若是选择“确定”，会将所有的设定清除，并重新开机。我们建议在做版本升级前请先将Router现在的设定值存在计算机，等做完版本升级后，使用此功能将机器做出厂值设定以确保机器升级

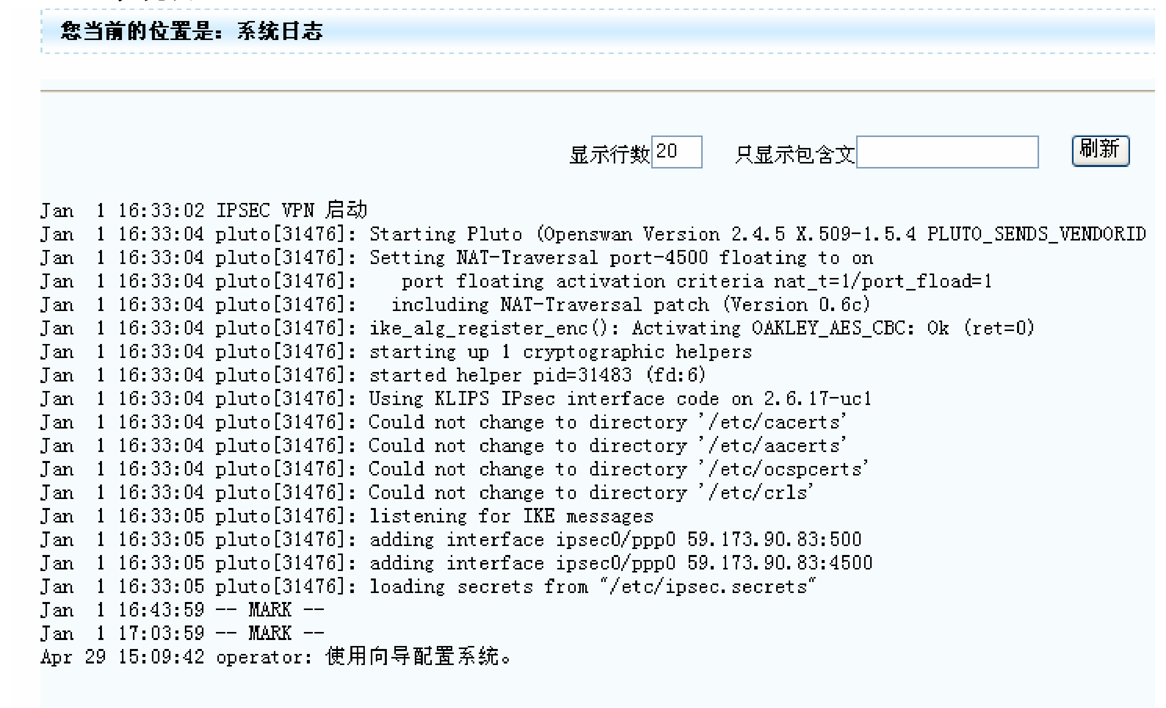
后的稳定行，然后再将刚才存在计算机的设定值存回(如何储存设定数据及升级完成后如何存回，请参考“配置备份与恢复”说明)。

4.3.8 配置向导

此项可以帮助用户通过一步到位的方式配置一些简单的路由器信息，实现路由器能够正常上网。具体步骤如下：

- 第一步：向导使用说明
- 第二步：选择系统模式，当前设置只支持网关模式。
- 第三步：选择WAN口的接入方式，此设置向导只支持对WAN1口的设置向导，如需其他WAN口的设置，请到4.3.2.2中进行设置。
- 第四步：如选择ADSL拨号，填写用户名和密码。如其他方式，填写对应的信息。
- 第五步：选择性设置WAN口带宽
- 第六步：定义内网配置信息
- 第七步：DHCP服务器配置，配置是否打开DHCP服务器，以及DHCP分配的信息。
- 第八步：点击完成重启路由器，实现配置。

4.3.9 系统日志



系统日志：提供了外部系统日志服务器收集系统信息功能。Syslog为一项工业标准通讯协议，网络上动态撷取有关的系统信息。系统日志提供了包含动作中的联机来源位置(Source IP Address)与目地(Destination IP Address)位置，服务编号(Port Number)以及型态(IP service)。输入您要查看的相关系统日志的服务器名称或是IP地址于“系统日志服务器”的空格字段内，您就可以查询到与此IP或者该信息相关的系统日志。

4.3.10 修改帐号

当您每次登入至路由的设定画面时，必须输入密码。密码出厂值为“888888”。为了安全理由，我们建议您务必在第一次登入并完成设定之后更改管理密码！密码请牢记，若是密码忘记，将无法再登入至路由器的设定画面，必须回复到出厂值(Factory Default)。

您当前的位置是：修改登录密码

修改登录密码

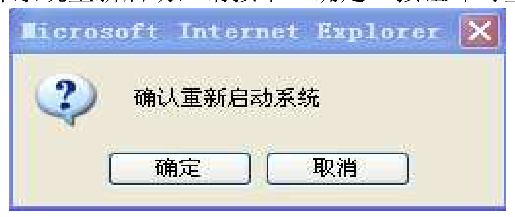
确认登录密码

修改

- 修改登录密码：填写所更改密码。
- 确认登录密码：再填写一次更改密码。
- 修改：按下此按钮“修改”即会储存修改的密码。
- 密码最高只支持8位。

4.3.11 重新启动

您可以在此工具中选择系统重新启动，请按下“确定”按钮即可重新启动路由器。



4.3.12 退出

您点击退出后，可以安全退出WEB管理界面。

附　　录

一、静态路由设置

下面就以几个典型应用为例，来说明一下什么情况需要设置静态路由，静态路由条目的组成，以及静态路由的具体作用。

例一：最简单的串连式双路由器型环境

这种情况多出现于中小企业在原有的路由器共享Internet的网络中，由于扩展的需要，再接入一台路由器以便连接另一个新加入的网段。而家庭中也很可能出现这种情况，如用一台宽带路由器共享宽带后，又加入了一台无线路由器满足无线客户端的接入。

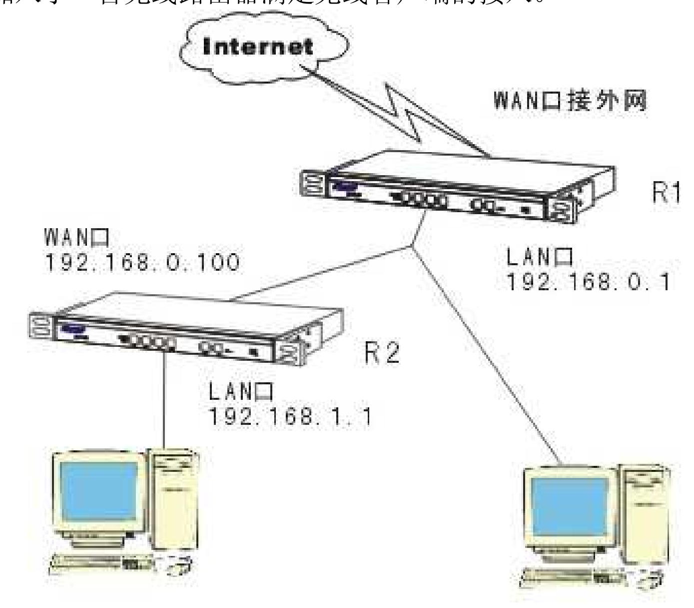


图1

（注：图中省略了可能存在的交换层设备）

如图1所示，LAN 1为192.168.0.0这个标准C类网段，路由器R1为原有路由器，它的WAN口接入宽带，LAN口（IP为192.168.0.1）挂着192.168.0.0网段（子网掩码255.255.255.0的C类网）主机和路由器R2（新添加）的WAN口（IP为192.168.0.100）。R2的LAN口（IP为192.168.1.1）下挂着新加入的LAN 2这个192.168.1.0的C类不同网段的主机。

如果按照共享Internet的方式简单设置，此时应将192.168.0.0的主机网关都指向R1的LAN口（192.168.0.1），192.168.1.0网段的主机网关指向R2的LAN口（192.168.1.1），那么只要R2的WAN口网关指向192.168.0.1，192.168.1.0的主机就都能访问192.168.0.0网段的主机并能通过宽带连接上网。这是因为前面所说的宽带路由器中一条默认路由在起作用，它将所有非本网段的目的IP包都发到WAN口的网关（即路由器R1），再由R1来决定信息包应该转发到它自己连的内网还是发到外网去。但是192.168.0.0网段的主机网关肯定要指向192.168.0.1，而R1这时并不知道192.168.1.0这个LAN 2的正确位置，那么此时只能上网以及本网段内的互访，不能访问到192.168.1.0网段的主机。这时就需要在R1上指定一条静态路由，使目的IP为192.168.1.0网段的信息包能转发到路由器R2去。

一条静态路由条目一般由3部分组成：1.目的IP地址或者叫信宿网络、子网；2.子网掩码；3.网关或叫下一跳。

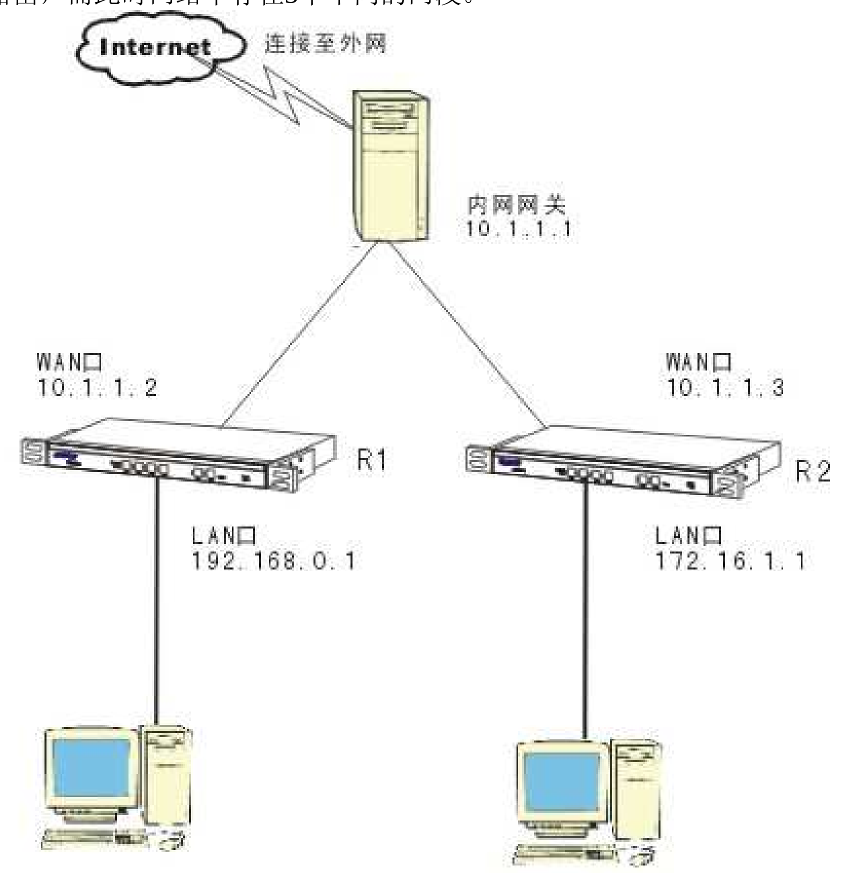
例1中R1上设定的静态路由条目就应该为：目的IP地址192.168.1.0（代表1.x这个网段），子网掩码255.255.255.0（因为是C类网段），下一跳192.168.0.100。如图2，此图为静态路由表配置项，保存后即可生效。

注意：其中的网关IP必须是与WAN或LAN口属于同一个网段。那条默认路由写出来就是：目

的IP为 0.0.0.0，子网掩码0.0.0.0，下一跳为WAN口上的默认网关，有时我们也称它为“8个0的默认路由”。另外，如果目的IP是一个具体的主机IP（如192.168.1.2），那么路由条目应为：目的IP 192.168.1.2，子网掩码255.255.255.255，下一跳或网关192.168.0.100。

例二：两台平级并连的路由器，下挂子网中主机需要互相通信的环境

这种情况，两台平行并连的路由器上层应该还有一个总的出口网关，而这个网关有可能因某种原因不便设置路由，而此时网络中存在3个不同的网段。



图中内网网关就是小区的网关，R1和R3分别为两户的宽带路由器，它们之间一般通过楼层的接入交换机和小区的骨干交换机连接在一起，此图省略了这一部分。图4的这种情况，只要在网关设备上按例一的方式添加两条路由就能实现两个子网中主机的互访，而且其10.0.0.0这个A类网段中存在的主机也都能通过这两条路由访问到R1和R3下的内网机。但是如果是小区的网关设备，那肯定是不会让用户随便配置路由条目的，而且您应该也不想小区内的所有用户都能直接访问到您的内网主机。这时，我们可以在R1和R3上各添加一条路由指向对方来实现R1和R3下主机直接互访的效果。

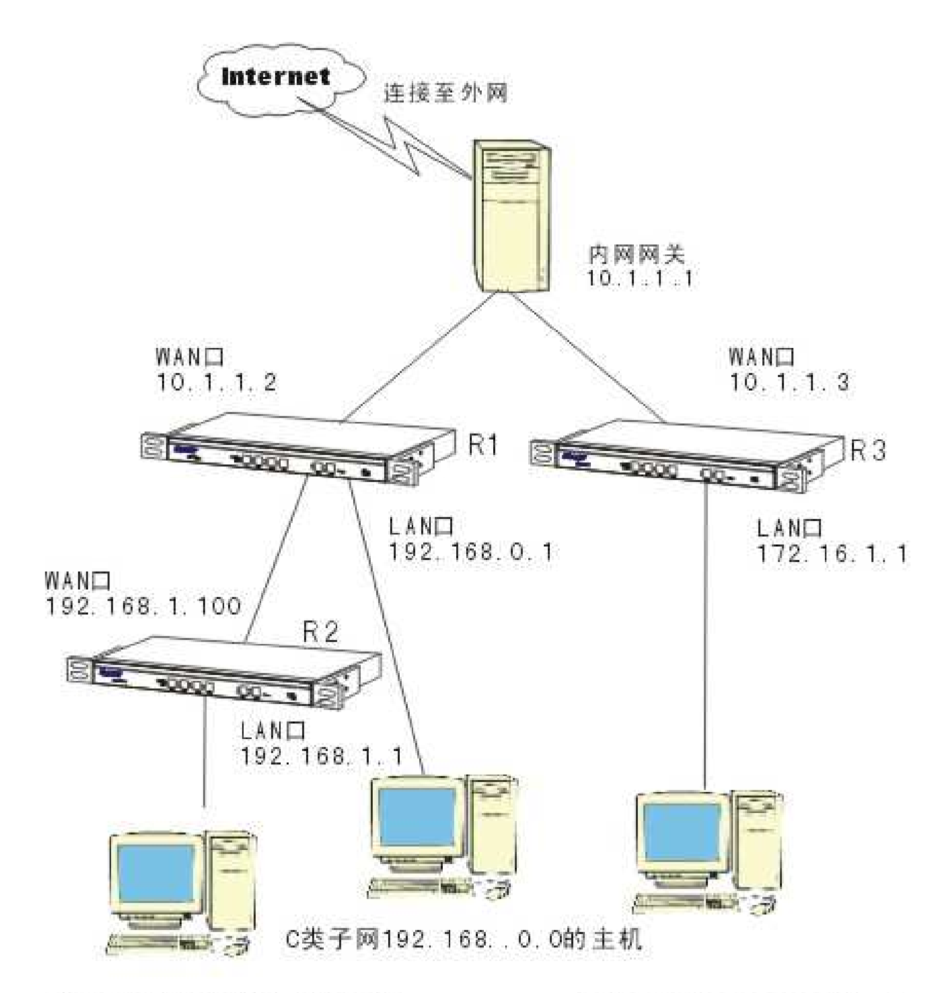
在R1上：目的IP地址172.16.0.0，子网掩码255.255.0.0（B类网段），下一跳10.1.1.3

在R3上：目的IP地址192.168.0.0，子网掩码255.255.255.0（C类网段），下一跳10.1.1.2

注：有些新型小区中使用了P-VLAN技术，这种网络的情况比较复杂，这样上面简单的静态路由设置有可能无法达到目的。

例三：既串且并，网络中有多级路由设备的环境。

这种情况可以说是例一和例二两种应用的整合和延伸，看似复杂其实简单



C类子网192.168.1.0的主机　　　　　　B类子网172.16.0.0的主机

既然拓扑图是例一、例二的结合，那将例一、例二中的路由条目加在一起是不是就可以了呢？当然也不是这么简单，如果只是配置了前两例的路由条目，R3下的主机是无法直接访问到R2下的192.168.1.0这个子网的。所以在R3上还要加一条到192.168.1.0这个子网的路由。静态路由条目配置如下：

R1：目的IP地址192.168.1.0，子网掩码255.255.255.0，下一跳192.168.0.100。

目的IP地址172.16.0.0，子网掩码255.255.0.0，下一跳10.1.1.3。

R3：目的IP地址192.168.0.0，子网掩码255.255.255.0，下一跳10.1.1.2。

目的IP地址192.168.1.0，子网掩码255.255.255.0，下一跳10.1.1.2。

如例三中，R3上的第一条：目的IP为192.168.0.0；第二条：目的IP为192.168.1.0。我们只提取了前面的两段192.168，而后面的第三段网络位中还是有相同的部分的。192.168.0.0中第三段写成二进制数为00000000（8位0），182.168.1.0中第三段写成二进制数为00000001（7位0，1位1），那么它们的前7位是相同的，在对应的子网掩码位置上就应该是11111110（7位1，1位0），合成十进制为254。所以这条汇总路由应该写成：目的IP为192.168.0.0，子网掩码255.255.254.0，下一跳10.1.1.2。这样，这条汇总路由只包含192.168.0.0和192.168.1.0两个子网，是一条精确的汇总路由。如图6中，R3下172.16.0.0的主机发送到192.168.2.0网段的信息包，其第三段网络位写成二进制为00000010（前6位0），就不包含在这条精确的汇总路由内了。

这时我们在R3上静态路由条目应该为

1.目的IP地址192.168.0.0，子网掩码255.255.254.0，下一跳10.1.1.2。

2.目的IP地址192.168.2.0，子网掩码255.255.255.0，下一跳10.1.1.4。

二、分位表示法 子网掩码

分位表示法	子网掩码
1	128.0.0.0
2	192.0.0.0
3	224.0.0.0
4	240.0.0.0
5	248.0.0.0
6	252.0.0.0
7	254.0.0.0
8	255.0.0.0
9	255.128.0.0
10	255.192.0.0
11	255.224.0.0
12	255.240.0.0
13	255.248.0.0
14	255.252.0.0
15	255.254.0.0
16	255.255.0.0
17	255.255.128.0
18	255.255.192.0
19	255.255.224.0
20	255.255.240.0
21	255.255.248.0
22	255.255.252.0
23	255.255.254.0
24	255.255.255.0
25	255.255.255.128
26	255.255.255.192
27	255.255.255.224
28	255.255.255.240
29	255.255.255.248
30	255.255.255.252
31	255.255.255.254
32	255.255.255.255